International Professional Practices Framework

Supplemental Guidance
Practice Guide

Internal Audit and the Second Line of Defense

The Institute of Internal Auditors | Global

Table of Contents

Executive Summary

As governance and monitoring functions collaborate more closely to avoid duplication of effort, internal audit may be asked to take on responsibilities for risk management, compliance, regulatory oversight, and other governance activities.

The chief audit executive (CAE) plays a critical role in navigating between internal audit's traditional role and assuming responsibilities for risk management, compliance, and other governance functions. The CAE should be held accountable for preserving independence and objectivity, communicating with management and the board, and confirming management's acceptance of risk to internal audit's independence and/or auditor objectivity. To navigate through these competing challenges, internal auditors can look to The IIA's guidance on effective risk management and control, and promulgated standards related to independence and objectivity.

Introduction

In January 2013, The IIA issued the Position Paper, The Three Lines of Defense in Effective Risk Management and Internal Control. The position paper outlines risk and control responsibilities within organizations and states that if dual responsibilities are assigned to a single person or department, consideration should be given to separating these functions at a later time. However, business constraints or other considerations may limit total separation among governance functions. This practice guide provides guidance to ensure independence and objectivity are not compromised in situations where internal audit may be responsible for second line of defense functions.

This guidance is not applicable where country and/or industry-specific standards may prohibit internal audit from performing second line of defense activities.

Business Significance and Related Risks

When following the Three Lines of Defense model, responsibilities among various functions of the organization are generally classified as follows:

- First line of defense: operational management functions that own and manage risks.
- Second line of defense: risk management and compliance functions that monitor risks.
- Third line of defense: an internal audit function that provides independent assurance.

When internal audit is also responsible for second line of defense functions, such as risk management and compliance, it is essential to implement safeguards to protect independence and/or objectivity and to routinely validate that the safeguards are operating effectively.

Management and the board should clearly understand the risks and appropriate controls needed when internal audit undertakes second line of defense functions.

Related IIA Standards

The following standards from the *International Standards for the Professional Practice of Internal Auditing* (Standards) relate to internal audit assuming second line of defense functions. Additional related IIA guidance documents are identified in Resources.

1100 – Independence and Objectivity

The internal audit activity must be independent, and internal auditors must be objective in performing their work.

1110 – Organizational Independence

The chief audit executive must report to a level within the organization that allows the internal audit activity to fulfill its responsibilities. The chief audit executive must confirm to the board, at least annually, the organizational independence of the internal audit activity.

1120 – Individual Objectivity

Internal auditors must have an impartial, unbiased attitude and avoid any conflict of interest.

1130 – Impairment to Independence or Objectivity

If independence or objectivity is impaired in fact or appearance, the details of the impairment must be disclosed to appropriate parties. The nature of the disclosure will depend upon the impairment.

> 1130.A1 – Internal auditors must refrain from assessing specific operations for which they were previously responsible. Objectivity is presumed to be impaired if an internal auditor provides assurance services for an activity for which the internal auditor had responsibility within the previous year.
>
> 1130.A2 – Assurance engagements for functions over which the chief audit executive has responsibility must be overseen by a party outside the internal audit activity.
>
> 1130.C1 – Internal auditors may provide consulting services relating to operations for which they had previous responsibilities.
>
> 1130.C2 – If internal auditors have potential impairments to independence or objectivity relating to proposed consulting services, disclosure must be made to the engagement client prior to accepting the engagement.

1322 – Disclosure of Nonconformance

When nonconformance with the Definition of Internal Auditing, the Code of Ethics, or the *Standards* impacts the overall scope or operation of the internal audit activity, the chief audit executive must disclose the nonconformance and the impact to senior management and the board.

2050 – Coordination

The chief audit executive should share information and coordinate activities with other internal and external providers of assurance and consulting services to ensure proper coverage and minimize duplication of efforts.

2100 – Nature of Work

The internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach.

2500 – Monitoring Progress

The chief audit executive must establish and maintain a system to monitor the disposition of results communicated to management.

> 2500.A1 – The chief audit executive must establish a follow-up process to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.
>
> 2500.C1 – The internal audit activity must monitor the disposition of results of consulting engagements to the extent agreed upon with the client.

2600 – Communicating the Acceptance of Risks

When the chief audit executive concludes that management has accepted a level of risk that may be unacceptable to the organization, the chief audit executive must discuss the matter with senior management. If the chief audit executive determines that the matter has not been resolved, the chief audit executive must communicate the matter to the board.

Definition of Key Concepts

Assurance Functions – Functions that provide assurance on the effectiveness of governance, risk management, and control.

Assurance Services – An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, system security, and due diligence engagements.[1]

[1] The International Profession Practices Framework (IPPF), pp. 42-43. 2013.

Board – The highest level of governing body charged with the responsibility to direct and/or oversee the activities and management of the organization. Typically, this includes an independent group of directors (e.g., a board of directors, a supervisory board, or a board of governors or trustees). If such a group does not exist, the "board" may refer to the head of the organization. "Board" may refer to an audit committee to which the governing body has delegated certain functions.[2]

Chief Audit Executive – Chief audit executive (CAE) describes a person in a senior position responsible for effectively managing the internal audit activity in accordance with the internal audit charter and the Definition of Internal Auditing, the Code of Ethics, and the *Standards*. The chief audit executive or others reporting to the chief audit executive will have appropriate professional certifications and qualifications. The specific job title of the chief audit executive may vary across organizations.[3]

Impairment – Impairment to organizational independence and individual objectivity may include personal conflict of interest, scope limitations, restrictions on access to records, personnel, and properties, and resource limitations (funding).[4]

Independence – The freedom from conditions that threaten the ability of internal audit to carry out internal audit responsibilities in an unbiased manner.[5]

Internal Audit Activity – A department, division, team of consultants, or other practitioner(s) that provides independent, objective assurance and consulting services designed to add value and improve an organization's operations. The internal audit activity helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management, and control processes.[6], [7]

Objectivity – An unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they believe in their work product and that no quality compromises are made. Objectivity requires that internal auditors do not subordinate their judgment on audit matters to others.[8]

[2] Ibid.
[3] Ibid.
[4] Ibid.
[5] Ibid.
[6] Ibid.
[7] Note: the terms "internal audit" and "internal audit activity" are used interchangeably in this practice guide.
[8] Ibid.

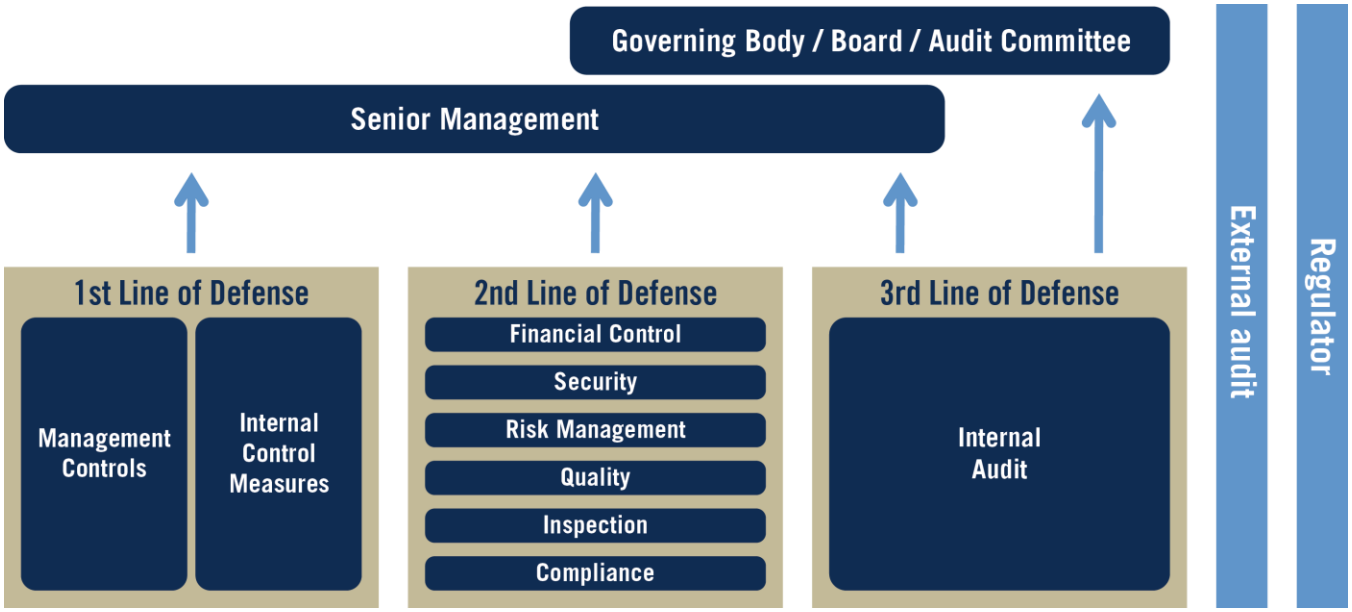
Overview of Good Governance

The Three Lines of Defense Model

The Three Lines of Defense model[9], as illustrated in Figure 1, describes responsibilities for effective risk management and control as follows:

- Management is primarily responsible for monitoring and controlling processes, and is the first line of defense in risk management.
- The second line of defense consists of separately established risk, control, and compliance oversight functions that ensure properly designed processes and controls are in place within the first line of defense and are operating effectively. The nature and types of these functions are dependent on many factors including industry and organizational maturity.
- Functions, such as internal audit, that provide independent assurance over processes and controls are considered the third line of defense.

Figure 1



Assuming effectiveness, each line of defense contributes to healthy organizational governance by ensuring objectives are achieved in the context of the social, regulatory, and market environments. Both the second and third lines provide oversight and/or assurance over risk

[9] The IIA's Position Paper, The Three Lines of Defense in Effective Risk Management and Control, 2013.

management. The key differences between the second and third lines of defense are the concepts of independence and objectivity.

Independence and Objectivity

Standard 1100 states that the internal audit activity must be independent, and internal auditors must be objective in performing their work. Conditions that threaten the ability of any organizational function, including internal audit, to perform its responsibilities in an unbiased manner have the potential to compromise independence and objectivity.

According to the interpretation of Standard 1110, organizational independence is effectively achieved when the chief audit executive reports functionally to the board, which includes board approval of the appointment, remuneration, and removal of the chief audit executive. Leaders in the second line of defense typically report functionally to organizational management and as a result, the second line of defense is not considered independent.

Benefits can be derived by an organization when the second and third lines of defense collaborate. Standard 2050 states that the chief audit executive should share information and coordinate activities with other internal and external providers of assurance and consulting services to ensure proper coverage and minimize duplication of efforts. The IIA's Practice Guide, Coordinating Risk Management and Assurance, provides guidance to the CAE on effective coordination and reporting so that resources are used effectively and key risks are not missed or misjudged.

Boards and management rely on internal audit to provide assurance on the adequacy of governance, risk management, and controls. This reliance is enhanced by internal audit's independence and internal auditors' objectivity. As governance and risk management activities expand, additional safeguards and controls are needed to maintain independence and objectivity.

Role of the CAE

Organizational Governance and Three Lines of Defense

In accordance with Standard 2100, internal audit must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach. If certain second line of defense functions are deemed critical to monitoring and/or providing assurance on the effectiveness of risk management and internal control, the CAE must evaluate the effectiveness of those functions relative to this objective. The scope of the evaluation will be driven by risk and the extent of reliance placed on these functions.

The IIA's Practice Guide, Reliance by Internal Audit on Other Assurance Providers, provides guidance to the CAE on an approach for relying on the assurance provided by other internal or external assurance functions, which is useful for assessing the effectiveness of the function.

Identifying Gaps and Potential Conflicts Within the Three Lines of Defense

When assessing second line of defense functions, the CAE may identify gaps, conflicts, or duplication of efforts. Consistent with Standard 2100, the CAE should work with stakeholders to recommend enhancements that improve governance, risk management, and internal controls. Outcomes may include collaborating between organizational areas to reduce overlap between functions and segregating responsibilities to properly maintain independence and objectivity. The following sections provide guidance to the CAE on maintaining independence and objectivity in situations where internal audit assumes second line of defense responsibilities.

Internal Audit and Second Line of Defense Responsibilities

Second Line of Defense Functions

Many organizations have asked or required the CAE to assume additional second line of defense responsibilities. This is often due to the size or maturity of the organization, or the result of new risk management or compliance initiatives undertaken by the organization. If not managed properly, objectivity, which is crucial to providing assurance to management and the board, could be impaired.

Regulatory standards and widely adopted industry practices may require specific second line of defense activities, such as risk management coordination or compliance review. For example, second line of defense responsibilities could be related to requirements for the

financial services industry, independent audits of quality management systems (ISO 9001), European Commission's Eco-Management and Audit Scheme (EMAS) to evaluate and report environmental performance, and United States Occupational Safety and Health Administration's (OSHA) enforcement of work-related health and safety rules.

Internal Audit and Second Line of Defense Activities

Responsibilities may become blurred across internal audit and second line of defense functions, even in organizations with robust risk management and governance programs and resources to support both. The CAE may be asked to assume second line of defense activities in situations such as:

- New regulatory requirement: A new regulation requires substantial effort associated with new policies, procedures, testing, and risk management activities.
- Change in business: An organization may enter into a new geographical market or new business segment and be subject to new regulations or risk management activities.
- Resource constraints: An organization may experience resource constraints or changes in staff, such as when the leader of a second line of defense function leaves the organization.
- Efficiency: Management and/or the board may determine it is more efficient for internal audit to perform compliance or other second line of defense functions.

Internal audit may be the preferred choice due to its expertise in applying risk management and governance principles in existing, new, and emerging areas. As an example, management across many organizations asked internal audit to take the lead compliance role when Sarbanes-Oxley legislation became required for U.S. public companies. The blending of internal audit with second line of defense activities may also occur without additional regulatory requirements or resource constraints, as management may determine that internal audit is the best fit for certain activities, such as where:

- The organization is small and cannot support distinct control and assurance functions.
- Management and the board do not believe the degree of risk warrants separate functions for certain second and third line of defense activities.
- Internal audit has the necessary skill set or relevant expertise for specific risk management and/or compliance responsibilities.
- Management and/or the board do not understand or appropriately value the importance of an independent and objective third line of defense.
- Internal audit responds to cost-cutting pressures or other factors, and assumes responsibilities for the good of the organization.

If second line of defense responsibilities are assumed by internal audit, the CAE should communicate the risks to management and the board. It is important for the CAE, management, and the board to understand the risks involved with assuming such duties, regardless of whether it will be a temporary or long-term arrangement. Either way, proper safeguards and controls need to be agreed upon, implemented, and periodically validated to ensure that internal audit's objectivity is properly maintained.

Safeguards to Maintain Independence and Objectivity

Corporate governance arrangements vary considerably among organizations, depending on factors such as the size of the organization, industry sector, availability of resources, culture, risk tolerance, make-up of the board, and the relative risk and importance of certain second line of defense activities to the entity. The effectiveness of internal audit's primary function — to provide independent, objective assurance and consulting services — should be protected. Any impairment to independence and/or objectivity needs to be elevated and evaluated.

Discussions on Dual Responsibilities

Standard 1110 requires confirmation to the board, at least annually, about the status of the internal audit function regarding organizational independence. Standard 1130 requires the disclosure of any impairment, in fact or appearance, to appropriate parties. The nature of the disclosure will depend on the impairment and should state the following:

- Situation.
- Consequences and risks to internal audit's independence and objectivity.
- Safeguards.
- Transition plan, if applicable.

Safeguards to Maintain Independence and Objectivity

If management and the board accept the risk of internal audit assuming second line of defense activities, safeguards and controls need to be put in place to ensure independence and objectivity are not compromised. The safeguards noted below should be considered for each second line of defense activity assigned to internal audit.

- Discussion of risks with management and the board.
- Acceptance and ownership of the risks by management.
- Clear definition and assignment of roles for each activity where second line of defense activities overlap with third line of defense activities, including the following documented components:
    - Impact and risks to the organization and internal audit.

    - Roles, responsibilities, and segregation of duties.
    - Controls put in place to validate that agreed upon safeguards are operating effectively.
    - Determination of whether the assignment is temporary or long-term.
        - If temporary, a transition plan is needed (see next section).
    - Documented acceptance and approval by senior management and the board.
    - Second line of defense activities performed by internal audit should be referenced in the charter and/or included in the board update, at least annually.
- Periodic (at least annual) evaluation of reporting lines and responsibilities by management and the board.
- The nature of internal audit's roles should be clearly stated in the audit charter.
- Periodic independent assessment of internal audit's second line of defense roles and the efficacy of the independence, objectivity, and assurance provisions.
    - The CAE should include a review of internal audit's second line of defense roles, in conjunction with its quality assurance and improvement program or on a more frequent basis, depending on the level of risk.
- Where safeguards to maintain internal audit's independence and objectivity are not possible, the *Standards* requires that responsibility for performing the second line of defense activity be reassigned elsewhere in the organization or outsourced to a third-party provider.

Internal audit should take care to avoid activities that compromise their independence and/or objectivity, including:

- Setting the risk appetite.
- Owning or managing risks.
- Assuming responsibilities for accounting, business development, and other first line of defense functions.
- Making risk response decisions on management's behalf.
- Implementing or assuming accountability for risk management or governance processes.
- Providing assurance on second line of defense activities performed by internal audit.

Transition Plan

If the assignment of second line of defense responsibilities to internal audit is deemed to be temporary, a formal transition plan to relieve internal audit from such responsibilities should be developed, discussed with management and the board, and implemented.

The transition plan should consider matters such as:

- Organizational/structural needs: Internal audit may need to adjust reporting relationships as individuals or groups cease their role in second line of defense activities. If these responsibilities are moving elsewhere in the organization, structural changes may be required to ensure independence and objectivity.
- Resources: Resources may be required to train individuals elsewhere in the organization for second line of defense duties or to transition internal audit staff to these roles.
- Timeline and tasks: Responsibilities and target dates for key milestones should be documented.
- Maintaining independence during transition: In accordance with Standard 1130.A1, individuals must refrain from assessing specific matters for which they were previously responsible for a period of at least one year. This would apply to individuals who have been involved in second line of defense activities while working within internal audit.
- Monitoring progress: The CAE should monitor progress of the transition plan.
- Transparency: Ongoing communication with management and the board regarding adherence to the transition plan and schedule. Significant changes or delays should be evaluated and approved by the board.

Internal audit's audit plan may include provisions to validate the completeness and effectiveness of the transition of second line of defense duties to the identified resources (a third party may need to lead this audit effort due to independence and objectivity implications). During the development and implementation of the transition plan, the CAE, along with senior management and the board, should consider the long-term organizational structure to ensure proper tone at the top; appropriateness of corporate governance programs; statutory, regulatory, and other mandatory compliance requirements; risk management culture; alignment with the three lines of defense approach; and the size and complexity of the organization.

Management's Acceptance of Risks to Independence and Objectivity

Organizations may opt to keep certain second line of defense responsibilities integrated within internal audit. This may occur in smaller organizations, as well as areas where management has concluded there is minimal risk or impact to the organization. The decision to integrate second and third lines of defense responsibilities as a longer-term strategy should be thoughtful, deliberate, and based on a risk analysis and substantial discussion with management and the board.

Management's acceptance of risks associated with blending internal audit with second line of defense activities may be regarded as suitable for a period of time, but it should not be regarded as permanent. Changes to the business, regulatory landscape, and underlying risks (either the inherent risks or application of risks on the business) can overwhelm the resources allocated to risk management. An evaluation, including a refresh of the risk analysis, should occur with management and the board at least annually to evaluate internal audit's current role in performing second line of defense activities.

The overlap of second and third line of defense activities is an excellent focus area for a quality assurance and improvement program. Internal audit should reassess the risks to independence and objectivity, communicate these to management, consider transition plans, and obtain management's acceptance of these risks on a periodic basis. The CAE may also ask external assessors to include such matters in the scope of their assessments.

As governance and risk management activities continue to evolve, internal audit may be asked or required by management to assume second line of defense responsibilities. Management and the board should evaluate, discuss, and accept the associated risks before blending these duties. The CAE should ensure that appropriate safeguards and controls, identified in this guidance, are implemented and periodically validated to maintain internal audit's independence and objectivity.

Resources

Related IIA Guidance

Following are IIA resources that may be useful for internal auditors to reference when faced with taking on responsibilities for risk management, compliance, regulatory oversight, and other governance activities.

Practice Advisory 2050-1: Coordination

Practice Advisory 2500.A1-1: Follow-up Process

The IIA's Practice Guide, Coordinating Risk Management and Assurance, 2012

The IIA's Practice Guide, Reliance by Internal Audit on Other Assurance Providers, 2011

The IIA's Position Paper, Three Lines of Defense in Effective Risk Management and Control, 2013.

Authors

Caroline Glynn, CIA

Douglas Hileman, CRMA, CPEA

Hans-Peter Lerchner, CIA

Thomas Sanglier, CIA, CRMA

About The IIA

The Institute of Internal Auditors (The IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 180,000 members from more than 170 countries and territories. The association's global headquarters are in Altamonte Springs, Fla. For more information, visit www.globaliia.org or www.theiia.org.

About Supplemental Guidance

Supplemental Guidance is part of The IIA's International Professional Practices Framework (IPPF) and provides additional recommended (non-mandatory) guidance for conducting internal audit activities. While supporting the *Standards*, Supplemental Guidance is not intended to directly link to achievement of conformance with the *Standards*. It is intended instead to address topical areas, as well as sector-specific issues, and it includes detailed processes and procedures. This guidance is endorsed by The IIA through formal review and approval processes.

Practice Guides

Practice Guides are a type of Supplemental Guidance that provide detailed guidance for conducting internal audit activities. They include detailed processes and procedures, such as tools and techniques, programs, and step-by-step approaches, as well as examples of deliverables. As part of the IPPF guidance, conformance with Practice Guides is recommended (non-mandatory). Practice Guides are endorsed by The IIA through formal review and approval processes.

A Global Technologies Audit Guide (GTAG) is a type of Practice Guide that is written in straightforward business language to address a timely issue related to information technology management, control, or security.

For other authoritative guidance materials provided by The IIA, please visit our website at www.globaliia.org/standards-guidance or www.theiia.org/guidance.

Disclaimer

Copyright

January 2016